Application Notes for Configuring Avaya Aura®
Communication Manager R6.2 Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to support Completel UCM Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Completel UCM service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. Completel is a member of the DevConnect Service Provider program.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.
1. Introduction
These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Completel UCM service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with the Completel UCM service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results
The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Avaya SBCE. The enterprise site was configured to use the SIP Trunking service provided by Completel.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

2.1. Interoperability Compliance Testing
The interoperability test included the following:
• Incoming calls to the enterprise site from PSTN phones using the SIP Trunk provided by Completel, calls made to SIP and H.323 telephones at the enterprise
• Outgoing calls from the enterprise site completed via Completel to PSTN destinations, calls made from SIP and H.323 telephones
• Calls using the G.711A and G.729 codecs
• Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
• DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
• User features such as hold and resume, transfer, conference, call forwarding, etc
• Caller ID Presentation and Caller ID Restriction
• Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones
• Call coverage and call forwarding for endpoints at the enterprise site
• Transmission and response of SIP OPTIONS messages sent by Completel requiring Avaya response and sent by Avaya requiring Completel response

2.2. Test Results
Interoperability testing of the sample configuration was completed with successful results for the Completel UCM service with the following observations:
• Calls to busy destinations were handled by the network using a backwards transmission path to play an announcement as opposed to sending “486 Busy Here” to the enterprise.
• Calls to unassigned numbers were handled by the network using a backwards transmission path to an announcement as opposed to sending “404 Not Found” to the enterprise.
• When there were no matching codecs on outgoing calls, the network sent an SDP answer with T.38 instead of rejecting the call with “488 Not Acceptable Here”. The SDP answer was rejected by the CM so the issue has limited impact.
• RFC 2833 was not used by the network to handle DTMF on test calls to international destinations. DTMF was successfully tested on calls between the enterprise and national destinations.
• Ringback was not heard on calls forwarded to international destinations. Call forwarding to national destinations was tested successfully.
• On incoming fax calls, the enterprise correctly sent a re-INVITE to change the codec to T.38. However the network also sent a re-INVITE which was rejected by the network with a “491 Request Pending - another fax request in progress”. The network cleared the call when it received this message. This was resolved by using the SBC to change the 491 response to a 200 OK.
• Test fax calls to international destinations failed. They were successfully tested to national destinations.
• EC500 Confirmed answer calls were not successful. Although broken dial tone was heard, the connection was not made when the digits were pressed on the mobile phone.
• When the trunk was busy and 500 Service Unavailable (Signaling Resources Unavailable) sent from the CM, the network re-attempted the call a number of times resulting in a delay before a tone was heard.
• When the signalling link was out of service and 500 Service Unavailable (Signaling Resources Unavailable) sent from the Enterprise, the network re-attempted the call a number of times resulting in a delay before a tone was heard.

2.3. Support
For technical support on Completel products please visit the website at www.completel.fr or contact an authorized Completel representative.
3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Completel UCM service. Located at the Enterprise site is an Avaya Session Border Controller for Enterprise, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya A175 Desktop Video Device running Flare Experience (audio only), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone running on a laptop PC configured for SIP.

Figure 1: Test Setup Completel UCM to Avaya Enterprise
4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

<table>
<thead>
<tr>
<th>Equipment/Software</th>
<th>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avaya</strong></td>
<td></td>
</tr>
<tr>
<td>Dell PowerEdge R620 running Session Manager on VM Version 8</td>
<td>SM-6.3.2.0.632023-e50-00</td>
</tr>
<tr>
<td>Dell PowerEdge R620 running System Manager on VM Version 8</td>
<td>SMGR-6.3.0.8.5682-e50-64 (Build 5682)</td>
</tr>
<tr>
<td>Avaya S8800 Server running Communication Manager</td>
<td>R016x. 02.0.823.0-20199 (R6.2 SP4)</td>
</tr>
<tr>
<td>Avaya Session Border Controller Advanced for Enterprise Server</td>
<td>6.2.0.Q48</td>
</tr>
<tr>
<td>Avaya 1616 Phone (H.323)</td>
<td>1.302</td>
</tr>
<tr>
<td>Avaya 4621 Phone (H.323)</td>
<td>2.902</td>
</tr>
<tr>
<td>Avaya 96x0 Phone (H.323)</td>
<td>3.200</td>
</tr>
<tr>
<td>Avaya A175 Desktop Video Device (SIP)</td>
<td>Flare Experience Release 1.1.2</td>
</tr>
<tr>
<td>Avaya 9630 Phone (SIP)</td>
<td>R2.6 SP9</td>
</tr>
<tr>
<td>Avaya 9608 Phone (SIP)</td>
<td>R6.2 SP1</td>
</tr>
<tr>
<td>Avaya one–X® Communicator (H.323) on Lenovo T510 Laptop PC</td>
<td>6.1.8.06-SP8-40314</td>
</tr>
<tr>
<td>Analogue Handset</td>
<td>NA</td>
</tr>
<tr>
<td>Analogue Fax</td>
<td>NA</td>
</tr>
<tr>
<td><strong>Completel</strong></td>
<td></td>
</tr>
<tr>
<td>ACME Net-Net 4500 SBC</td>
<td>SCX6.2.0 MR-5 GA (Build 777)</td>
</tr>
<tr>
<td>Cirpack Softswitch</td>
<td>v4.2J14</td>
</tr>
</tbody>
</table>

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP signalling associated with the Completel UCM service. For incoming calls, the Session Manager receives SIP messages from the Avaya SBC for Enterprise (Avaya SBCE) and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Completel network. Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been
abridged and highlighted for brevity and clarity in presentation. The general installation of the Avaya S8800 Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the display system-parameters customer-options command and on Page 2, verify that the Maximum Administered SIP Trunks supported by the system is sufficient for the combination of trunks to the Complete network, and any other SIP trunks used.

<table>
<thead>
<tr>
<th>IP PORT CAPACITIES</th>
<th>USED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Administered H.323 Trunks: 12000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP Stations: 18000 3</td>
<td></td>
</tr>
<tr>
<td>Maximum Administered Remote Office Trunks: 12000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Concurrently Registered Remote Office Stations: 18000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP eCons: 414 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Video Capable Stations: 18000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Video Capable IP Softphones: 18000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Administered SIP Trunks: 24000 20</td>
<td></td>
</tr>
<tr>
<td>Maximum Number of DS1 Boards with Echo Cancellation: 522 0</td>
<td></td>
</tr>
<tr>
<td>Maximum TN2501 VAL Boards: 128 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Media Gateway VAL Sources: 250 1</td>
<td></td>
</tr>
<tr>
<td>Maximum TN2602 Boards with 80 VoIP Channels: 128 0</td>
<td></td>
</tr>
<tr>
<td>Maximum TN2602 Boards with 320 VoIP Channels: 128 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Number of Expanded Meet-me Conference Ports: 300 0</td>
<td></td>
</tr>
</tbody>
</table>
On Page 4, verify that IP Trunks field is set to y.

5.2. Administer IP Node Names
The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the IP Node Names form, assign the node Name and IP Address for Session Manager. In this case, SM-BGVM1 and 10.10.79.61 are the Name and IP Address for Session Manager SIP interface. Also note the procr name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.
5.3. Administer IP Network Region

Use the `change ip-network-region 1` command to set the following values:

- The **Authoritative Domain** field is configured to match the SIP domain name configured on Session Manager. In this configuration, the SIP domain name is `trusted.voip.completel.fr`.
- By default, **IP-IP Direct Audio** (both Intra- and Inter-Region) is enabled (`yes`) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set 1 is used.
- The UDP port values used for the RTP media stream are defined by **UDP Port Min** and **UDP Port Max**, during test these were set to values other than the default values, namely 10000 and 10201 respectively. Normally these can be left at default values.

```
change ip-network-region 1
IP NETWORK REGION
Region: 1
Location: 1
Authoritative Domain: trusted.voip.completel.fr
Name: default

MEDIA PARAMETERS
Codec Set: 1
Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
UDP Port Min: 10000
UDP Port Max: 10201

DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26

802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5

AUDIO RESOURCE RESERVATION PARAMETERS
RSVP Enabled? n

H.323 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```
5.4. Administer IP Codec Set

Open the IP Codec Set form for the codec set specified in the IP Network Region form in Section 5.3. Enter the list of audio codec’s eligible to be used in order of preference. For the interoperability test the codec’s supported by Completel were configured, namely G.711A and G.729A.

<table>
<thead>
<tr>
<th>Codec</th>
<th>Audio</th>
<th>Silence</th>
<th>Frames</th>
<th>Packet</th>
<th>Codec Suppression Per Pkt</th>
<th>Size (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: G.711A</td>
<td>n</td>
<td>2</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2: G.729A</td>
<td>n</td>
<td>2</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Completel UCM service supports T.38 for transmission of fax. Navigate to Page 2 to configure T.38 by setting the FAX - Mode to t.38-standard as shown below.

<table>
<thead>
<tr>
<th>FAX</th>
<th>Mode</th>
<th>Redundancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem</td>
<td>t.38-standard</td>
<td>0</td>
</tr>
<tr>
<td>TDD/TTY</td>
<td>US</td>
<td>3</td>
</tr>
<tr>
<td>Clear-channel</td>
<td>n</td>
<td>0</td>
</tr>
</tbody>
</table>
5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the CompleTel UCM service. During test, this was configured to use TLS (Transport Layer Security) and the default TLS port of 5061 which is recommended for security. However, if tracing and fault analysis is required it may be more convenient to use TCP and port 5060. Configure the Signaling Group using the `add signaling-group x` command as follows:

- **Set Group Type** to `sip`
- **Set Transport Method** to `tls`
- **Set Peer Detection Enabled** to `y` allowing Communication Manager to automatically detect if the peer server is a Session Manager
- **Set Near-end Node Name** to the processor interface (node name `procr` as defined in the IP Node Names form shown in Section 5.2)
- **Set Far-end Node Name** to Session Manager (node name `SM-BGVM1` as defined in the IP Node Names form shown in Section 5.2)
- **Set Near-end Listen Port** and **Far-end Listen Port** to `5061` (commonly used TLS port value)
- **Set Far-end Network Region** to the IP Network Region configured in Section 5.3. (logically establishes the far-end for calls using this signalling group as network region 1)
- **Leave Far-end Domain** blank (allows Communication Manager to accept calls from any SIP domain on the associated trunk)
- **Set Direct IP-IP Audio Connections** to `y`
- **Leave DTMF over IP** at default value of `rtp-payload` (Enables RFC2833 for DTMF transmission from Communication Manager)

The default values for the other fields may be used.

```
add signaling-group 2

SIGNALING GROUP

Group Number: 2                  Group Type: sip
IMS Enabled? n                   Transport Method: tls
Q-SIP? n                         
IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y        Peer Server: SM

Near-end Node Name: procr        Far-end Node Name: SM-BGVM1
Near-end Listen Port: 5061       Far-end Listen Port: 5061
                                   Far-end Network Region: 1

Far-end Domain:                  Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload        Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3 IP Audio Hairpinning? n
Enable Layer 3 Test? y           Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```
5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in Section 5.5. Configure the trunk group using the add trunk-group x command, where x is an available trunk group. On Page 1 of this form:

- Set the Group Type field to sip
- Choose a descriptive Group Name
- Specify a trunk access code (TAC) consistent with the dial plan
- The Direction is set to two-way to allow incoming and outgoing calls
- Set the Service Type field to public-netwrk
- Specify the signalling group associated with this trunk group in the Signaling Group field as previously configured in Section 5.5
- Specify the Number of Members supported by this SIP trunk group

```
add trunk-group 2
```

```
TRUNK GROUP
Group Number: 2                    Group Type: sip                CDR Reports: y
Group Name: VM SM                   COR: 1                      TN: 1        TAC: 102
Direction: two-way                  Outgoing Display? n          Night Service:
Dial Access? n                      Queue Length: 0
Service Type: public-netwrk         Auth Code? n                Member Assignment Method: auto
                                      Signaling Group: 2
                                      Number of Members: 10
```

On Page 2 of the trunk-group form, the Preferred Minimum Session Refresh Interval (sec) field should be set to a value mutually agreed with Completel to prevent unnecessary SIP messages during call setup.

```
add trunk-group 2
```

```
TRUNK PARAMETERS
Unicode Name: auto
Redirect On OPTIM Failure: 5000
SCCAN? n                             Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 300
Disconnect Supervision - In? y        Out? y
```

BG; Reviewed:  Solution & Interoperability Test Lab Application Notes  11 of 58
SPOC 12/4/2013   ©2013 Avaya Inc. All Rights Reserved.  CMPTL_CM62_SM63
On Page 3, set the **Numbering Format** field to **private**. This allows delivery of Calling Line Identity (CLI) with leading zeros and without a “+” prefix.

```
add trunk-group 2
TRUNK FEATURES

ACA Assignment? n  Measured: none
Maintenance Tests? y
Numbering Format: private
UUI Treatment: service-provider
Replace Restricted Numbers? n
Replace Unavailable Numbers? n
```

On Page 4 of this form:

- Set **Send Transferring Party Information** to **y**
- Set **Send Diversion Header** to **y**
- Set **Support Request History** to **n** as this is not required by the Service Provider
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Completel (this Payload Type is not applied to calls from SIP end-points)
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on the Communication Manager extension

```
add trunk-group 2

PROTOCOL VARIATIONS

Mark Users as Phone? n
Prepend ‘+’ to Calling Number? n
Send Transferring Party Information? y
Network Call Redirection? y
Send Diversion Header? y
Support Request History? n
Telephone Event Payload Type: 101

Convert 180 to 183 for Early Media? n
Always Use re-INVITE for Display Updates? n
Identity for Calling Party Display: From
Block Sending Calling Party Location in INVITE? n
Enable Q-SIP? n
```
5.7. Administer Calling Party Number Information

Use the `change private-unknown-numbering` command to configure Communication Manager to send the calling party number in national format with leading zero. In the test configuration, individual stations were mapped to send numbers allocated from the Completel Direct Dial-In (DDI) range supplied. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Note that the digits identifying the DDI range are not shown.

<table>
<thead>
<tr>
<th>Ext Ext</th>
<th>Trk</th>
<th>Private</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Len</td>
<td>Code</td>
<td>Grp(s)</td>
<td>Prefix</td>
</tr>
<tr>
<td>4</td>
<td>2000</td>
<td>2</td>
<td>02765nnn0</td>
</tr>
<tr>
<td>4</td>
<td>2298</td>
<td>2</td>
<td>02765nnn3</td>
</tr>
<tr>
<td>4</td>
<td>2316</td>
<td>2</td>
<td>02765nnn5</td>
</tr>
<tr>
<td>4</td>
<td>2346</td>
<td>2</td>
<td>02765nnn2</td>
</tr>
<tr>
<td>4</td>
<td>2396</td>
<td>2</td>
<td>02765nnn1</td>
</tr>
<tr>
<td>4</td>
<td>2402</td>
<td>2</td>
<td>02765nnn5</td>
</tr>
<tr>
<td>4</td>
<td>2611</td>
<td>2</td>
<td>02765nnn4</td>
</tr>
</tbody>
</table>

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the Completel UCM service. The single digit 9 was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the `change feature-access-codes` command to configure a digit as the Auto Route Selection (ARS) - Access Code 1.

| Abbreviated Dialing List1 Access Code: |
| Abbreviated Dialing List2 Access Code: |
| Abbreviated Dialing List3 Access Code: |
| Announcement Access Code: *69 |
| Answer Back Access Code: |
| Attendant Access Code: |
| Auto Alternate Routing (AAR) Access Code: 7 |
| Auto Route Selection (ARS) - Access Code 1: 9 |
| Access Code 2: |
Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0 or 00353. Calls are sent to **Route Pattern 2**.

**Note:** that exact maximum number lengths should be used where possible to reduce post-dial delay.

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Min</th>
<th>Total Max</th>
<th>Route Pattern</th>
<th>Call Type</th>
<th>ANI Num</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>14</td>
<td>2</td>
<td>pubu</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>00353</td>
<td>10</td>
<td>14</td>
<td>2</td>
<td>pubu</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>5</td>
<td>6</td>
<td>2</td>
<td>pubu</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>

Use the **change route-pattern** `x` command, where `x` is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern 2 is used to route calls to trunk group 2. CLI is set to a private format and the private numbering table used by setting the **Numbering Format** to `unk-unk`.

<table>
<thead>
<tr>
<th>Pattern Number: 2</th>
<th>Pattern Name: Calls via VM SM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grp FRL NPA Pfx Hop Toll No. Inserted</td>
<td>DCS/ IXC</td>
</tr>
<tr>
<td>No Mrk Lmt List Del Digits Dgts</td>
<td>QSIG Intw</td>
</tr>
<tr>
<td>1: 2 0</td>
<td>n user</td>
</tr>
<tr>
<td>2:</td>
<td>n user</td>
</tr>
<tr>
<td>3:</td>
<td>n user</td>
</tr>
<tr>
<td>4:</td>
<td>n user</td>
</tr>
<tr>
<td>5:</td>
<td>n user</td>
</tr>
<tr>
<td>6:</td>
<td>n user</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BCC VALUE</th>
<th>TSC</th>
<th>CA-TSC</th>
<th>ITC</th>
<th>BCIE Service/Feature PARM</th>
<th>No. Numbering</th>
<th>LAR Dgts Format</th>
<th>Subaddress</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 M 4 W Request</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>unk-unk</td>
</tr>
<tr>
<td>1: y y y y y n n</td>
<td>rest</td>
<td></td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2: y y y y y n n</td>
<td>rest</td>
<td></td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3: y y y y y n n</td>
<td>rest</td>
<td></td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4: y y y y y n n</td>
<td>rest</td>
<td></td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5: y y y y y n n</td>
<td>rest</td>
<td></td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6: y y y y y n n</td>
<td>rest</td>
<td></td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to Communication Manager extensions. The incoming digits sent in the INVITE message from Completel can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by Completel for testing are assigned to the internal extensions of the test equipment configured within Communication Manager. The `change inc-call-handling-trmt trunk-group x` command is used to translate numbers 02765nnnn0 to 02765nnnn5 to the 4 digit extension by deleting all (10) of the incoming digits and inserting the extension number.

Note: that the significant digits beyond the area code have been obscured.

```
change inc-call-handling-trmt trunk-group 2
```

5.10. EC500 Configuration

When EC500 is enabled on a Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2396. Use the command `change off-pbx-telephone station-mapping x` where x is the station in Communication Manager.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g. 0035386nnnnnnn)
- Set the **Trunk Selection** to 2 so that Trunk Group 2 will be used for routing
- Set the **Config Set** to 1

```
change off-pbx-telephone station-mapping 2396
```

Save Communication Manager changes by entering `save translation`.
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

6.1. Log in to Avaya Aura® System Manager

Access System Manager using a Web Browser by entering http://<FQDN>/SMGR, where <FQDN> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the Home tab will be presented with menu options shown below.
6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name agreed with Completel; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on the Communication Manager. Refer to **Section 5.3** for details. In test, **trusted.voip.completel.fr** was used. Optionally, a description for the domain can be entered in the Notes field (not shown). Click **Commit** to save changes.
6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu (not shown). Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row. Below is the location configuration used for the test enterprise.

**Note:** "*" is used to specify any number of allowed characters at the end of the string.
6.4. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select SIP Entities on the left panel menu, and then click on the New button (not shown). The following will need to be entered for each SIP Entity.

Under General:
- In the Name field enter an informative name
- In the FQDN or IP Address field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the Type field use Session Manager for a Session Manager SIP entity, CM for a Communication Manager SIP entity and SIP Trunk for Avaya SBCE SIP entity
- In the Location field select the appropriate location from the drop down menu
- In the Time Zone field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities:
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Session Border Controller for Enterprise (Avaya SBCE)

6.4.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The FQDN or IP Address field is set to the IP address of SIP signalling interface of Session Manager.
The Session Manager must be configured with the port numbers and transport protocols that will be used by the other SIP entities. To configure these, scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field, enter the port number on which the system listens for SIP requests.
- In the **Protocol** field, enter the transport protocol to be used for SIP requests.
- In the **Default Domain** field, from the drop down menu select the domain added in Section 6.2 as the default SIP domain.

### 6.4.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the location as defined in Section 6.3 and the **Time Zone** to the appropriate time zone.
6.4.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set the location as defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.
6.5. Administer Entity Links

A SIP trunk between Session Manager and another system is described by an Entity Link. To add an Entity Link, select Entity Links on the left panel menu and click on the New button (not shown). Fill in the following fields in the new row that is displayed.

- In the Name field enter an informative name
- In the SIP Entity 1 field select Session Manager
- In the Port field enter the port number to which the other system sends its SIP requests
- In the SIP Entity 2 field enter the other SIP Entity for this link, created in Section 6.4
- In the Port field enter the port number to which the other system expects to receive SIP requests
- Select the Trusted tick box to make the other system trusted
- In the Protocol field enter the transport protocol to be used to send SIP requests

Click Commit to save changes. The following screen shows the Entity Links used in this configuration.
6.6. Administer Routing Policies
Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select Routing Policies on the left panel menu and then click on the New button (not shown).

Under General:
- Enter an informative name in the Name field
- Under SIP Entity as Destination, click Select, and then select the appropriate SIP entity to which this routing policy applies
- Under Time of Day, click Add, and then select the time range

The following screen shows the routing policy for Communication Manager.
The following screen shows the routing policy for Avaya SBCE.

### 6.7. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:
- In the **Pattern** field enter a dialled number or prefix to be matched
- In the **Min** field enter the minimum length of the dialled number
- In the **Max** field enter the maximum length of the dialled number
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**

Under **Originating Locations and Routing Policies**:
- Click **Add**, in the resulting screen (not shown)
- Under **Originating Location**, select the location defined in **Section 6.3** or **ALL**
- Under **Routing Policies** select one of the routing policies defined in **Section 6.6**.
- Click **Select** button to save.
The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the Completel UCM service.

![Example dial pattern configured for the Avaya SBCE](image1)

The following screen shows the test dial pattern configured for Communication Manager.

![Test dial pattern configured for Communication Manager](image2)

**Note:** the pattern to be matched has been obscured.
6.8. Administer Application for Avaya Aura® Communication Manager

From the Home tab select Session Manager from the menu. In the resulting tab from the left panel menu select Application Configuration ➔ Applications and click New (not shown).

- In the Name field enter a name for the application
- In the SIP Entity field select the SIP entity for Communication Manager
- In the CM System for SIP Entity field select the SIP entity for Communication Manager and select Commit to save the configuration.

6.9. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to Session Manager ➔ Application Configuration ➔ Application Sequences and click on New (not shown).

- In the Name field enter a descriptive name
- Under Available Applications, click the + sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the Applications in this Sequence heading. Select Commit.
6.10. Administer SIP Extensions

SIP extensions are registered with Session Manager and use Communication Manager for their feature and configuration settings. From the Home tab select User Management from the menu. Then select Manage Users and click New (not shown).

On the Identity tab:

- Enter the user’s name in the Last Name and First Name fields
- In the Login Name field enter a unique system login name in the form of user@domain e.g. 2208@trusted.voip.completel.fr (entire name could not be displayed in the screenshot) which is used to create the user's primary handle
- The Authentication Type should be Basic
- In the Password/Confirm Password fields enter an alphanumeric password
- Set the Language Preference and Time Zone as required
On the Communication Profile tab, enter a numeric Communication Profile Password and confirm it.

Expand the Communication Address section and click New. For the Type field select Avaya SIP from the drop-down menu. In the Fully Qualified Address field, enter an extension number and select the relevant domain from the drop-down menu. Click the Add button.
Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** check box is checked.
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field.
- Select the appropriate application sequence from the drop-down menu in the **Origination Sequence** field configured in **Section 6.9**.
- Select the appropriate application sequence from the drop-down menu in the **Termination Sequence** field configured in **Section 6.9**.
- Select the appropriate location from the drop-down menu in the **Home Location** field.
Expand the **Endpoint Profile** section.

- Select the SIP Entity for Communication Manager from the **System** drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- In the **Port** field IP is automatically inserted
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box
- Select **Commit** (Not Shown) to save changes and System Manager will add the user configuration automatically to Communication Manager.
7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider’s SIP Trunk that is standard where possible and adapted to the Service Provider’s SIP implementation where necessary.

7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL https://<ip-address>, where <ip-address> is the private IP address configured at installation. A log in screen is presented. Log in using username ucsec and the appropriate password.

Once logged in, a dashboard is presented (not shown) with a menu on the left-hand side. The menu is used as a starting point for all administration of the Avaya SBCE.
7.2. Define Network Information

Network information is required on the Avaya SBCE to allocate IP addresses and netmasks to the interfaces. Note that only the A1 and B1 interfaces are used, typically the A1 interface is used for the internal side and B1 is used for external. Each side of the Avaya SBCE can have only one interface assigned.

To define the network information, navigate to Device Specific Settings ➔ Network Management in the main menu on the left-hand side and click on Add. Enter details in the blank box that appears at the end of the list:

- Define the internal IP address with netmask and assign to interface A1
- Select Save to save the information
- Click on Add
- Define the external IP address with netmask and assign to interface B1
- Select Save to save the information
- Click on System Management in the main menu
- Select Restart Application indicated by an icon in the status bar (not shown)

Select the Interface Configuration tab and click on Toggle State to enable the interfaces.
7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

7.3.1. Signalling Interfaces

To define the signalling interfaces on Avaya SBCE, navigate to Device Specific Settings ➔ Signaling Interface (not shown) in the main menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling interfaces are entered here:

- Select Add and enter details of the internal signalling interface in the pop-up menu (not shown)
- In the Name field enter a descriptive name for the internal signalling interface used for Session Manager
- For Signaling IP, select an internal signalling interface IP address defined in Section 7.2
- Select TCP port number 5060
- Select Add and enter details of the external signalling interface in the pop-up menu (not shown)
- In the Name field enter a descriptive name for the external signalling interface used for Completel
- For Signaling IP, select an external signalling interface IP address defined in Section 7.2
- Select UDP port number 5060
7.3.2. Media Interfaces

To define the media interfaces on Avaya SBCE, navigate to Device Specific Settings ➔ Media Interface in the main menu on the left hand side (not shown). Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

- Select Add and enter details of the internal media interface in the pop-up menu
- In the Name field enter a descriptive name for the internal media interface
- For Media IP, select an internal media interface IP address defined in Section 7.2
- Select RTP port ranges for the media path with the enterprise end-points
- Select Add and enter details of the external media interface in the pop-up menu
- In the Name field enter a descriptive name for the external media interface
- For Media IP, select an external media interface IP address defined in Section 7.2
- Select RTP port ranges for the media path with the Completel network

Note: during test the port ranges for the internal and external media interfaces were defined as the default values used by Communication Manager,
7.4. Define Server Interworking

Server interworking is defined for each server connected to Avaya SBCE. In this case, the Complete SBC is connected as the Trunk Server and Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

To define server interworking on Avaya SBCE, navigate to Global Profiles → Server Interworking in the main menu on the left hand side. To define Server Interworking for the Session Manager, highlight the avaya-ru profile which is a factory setting appropriate for Avaya equipment and select Clone Profile. A pop-up menu is generated headed Clone Profile (not shown)

- In the Clone Name field enter a descriptive name for the Session Manager and click Finish – in test ASM9 was used (not shown)
- In the General tab (not shown) Select Edit and enter details in the pop-up menu.
- Check the T.38 box then click Next and Finish (not shown)
• In the Advanced tab (not shown) Select Edit and enter details in the pop-up menu.
• Uncheck the AVAYA Extensions box

To define Server Interworking for the Completel SBC, highlight the previously defined profile for Session Manager and select Clone Profile. A pop-up menu is generated headed Clone Profile (not shown).
  • In the Clone Name field enter a descriptive name for server interworking profile for the Completel SBC and click Finish – in test Completel was used
  • Select Edit and enter details in the pop-up menu
  • Check the T.38 box
  • Select Next three times and click Finish

7.5. Define Signalling Manipulation

Signalling manipulation is required in some cases to ensure effective interworking. During test, an issue was found in the use of the UPDATE message between Completel UCM service and the enterprise that could not be resolved by other methods such as Server Interworking and Signaling Rules. The issue occurred when the UPDATE message was sent from the Completel network to change the codec to T.38 for fax calls. The enterprise was not successfully changing the codec and the fax calls were failing. The solution was to remove UPDATE from the Supported header in messages going from the enterprise to the network. This prompts the network to use re-INVITE instead of UPDATE.

To define the signalling manipulation to remove UPDATE from the Supported header in outgoing messages, navigate to Global Profiles ➔ Signaling Manipulation in the main menu on the left hand side. Click on Add Script and enter a title and the script in the script editor (not shown). The title in the example is Remove.UPDATE. The script text is as follows:
Once entered and saved, the script appears as shown in the following screenshot:

7.6. Define Servers

Servers are defined for each server connected to Avaya SBCE. In this case, the Completel SBC is connected as the Trunk Server and Session Manager is connected as the Call Server. To define Session Manager, navigate to Global Profiles ➔ Server Configuration in the main menu on the left hand side (not shown).
Click on **Add** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for Session Manager and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Call Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the SIP signalling interface of Session Manager. This is the same IP address as defined on Communication Manager in Section 5.2
- Check **TCP** in **Supported Transports**
- Define the **TCP** port for SIP signalling, **5060** is used for Session Manager and click **Finish**

![Server Configuration: ASM9_Call_Server](image)

- Select the **Advanced** tab (not shown)
- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for Session Manager as defined in Section 7.4
- In the **Signaling Manipulation Script** drop down menu, select the script defined in Section 7.5
- Click **Finish**

![Edit Server Configuration Profile - Advanced](image)
To define the CompleTel SBC as a Trunk Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side (not shown). Click on **Add** and enter details in the pop-up menu.

- In the **Profile Name** field enter a descriptive name for the CompleTel SBC and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Trunk Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the CompleTel SBC
- Check **UDP** in **Supported Transports**
- Define the **UDP** port for SIP signaling, **5060** is used for CompleTel

Click **Next** and check the **Enable Authentication** box
Define the Authentication parameters as provided by CompleTel.
Periodic REGISTER messages are required on the SIP trunk along with authentication for security. The REGISTER messages are defined using the heartbeat feature on Avaya SBCE. The heartbeat feature is defined in the Server configuration.

- Click **Next** and check the **Enable Heartbeat** box
- In the **Method** drop down menu, select **REGISTER**
- In the **Frequency** field, an arbitrary value of 3600 was set for test.
- In the **From URI** and **To URI** fields, use the username and domain as defined for authentication

Note: the REGISTER requests are sent at regular intervals defined by the expires parameter in the 200 OK response to the REGISTER request. The expires parameter is in the Contact Header of the 200 OK and during test was set to 45 (seconds). The interval defined in **Frequency** field in the above configuration does not have any effect on the timing of REGISTER requests.

- Click **Next** again then select the **Interworking Profile** for the Completer SBC defined in **Section 7.4** from the drop down menu
7.7. Define Routing

Routing information is required for routing to Session Manager on the internal side and the Completed SBC on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the Next Hop IP Address, default 5060 is used. To define routing to Session Manager, navigate to Global Profiles ➔ Routing in the main menu on the left hand side (not shown). Click on Add and enter details in the Routing Profile pop-up menu.

- In the Profile Name field enter a descriptive name for Session Manager, in this case Call Server, and click Next (not shown)
- Enter the IP address and port of the SIP signalling interface for Session Manager in the Next Hop Server 1 field
- Select TCP for the Outgoing Transport
- Click Finish

To define routing to the Completed SBC, navigate to Global Profiles ➔ Routing in the main menu on the left hand side (not shown). Click on Add and enter details in the Routing Profile pop-up menu.

- In the Profile Name field enter a descriptive name for the Completed SBC, in this case a generic name of Trunk Server was used, and click Next
- Enter the Completed SBC IP address and port in the Next Hop Server 1 field
- Select UDP for the Outgoing Transport
- Click Finish
7.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default Replace Action is Auto. This replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from Session Manager. In some cases where Topology Hiding can’t be applied, in particular the Contact header, IP addresses are translated to Avaya SBCE external addresses using NAT.
To define Topology Hiding for Session Manager, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side (not shown). Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for Session Manager and click **Next**
- If the **Request-Line**, **Record-Route** and **Via** Headers aren’t shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **To** and **SDP** Headers aren’t shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the “anonymous.invalid” domain name for restricted CLI is not overwritten)
- For each of the headers leave the **Replace Action** at the default value of **Auto**

![Topology Hiding Profiles: ASM9](image)

**Note:** the use of **Auto** results in an IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used where appropriate, and the required domain names entered in the **Overwrite Value** field. Different domain names can be used for the enterprise and the Completel network.
To define Topology Hiding for the Completel SBC, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side (not shown). Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the Completel SBC and click **Next**
- If the **Record-Route** and **Via** Headers aren’t shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **From** and **SDP** and **Request-Line** Headers aren’t shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the “anonymous.invalid” domain name for restricted CLI is not overwritten)
- For the **From** and **SDP** headers leave the **Replace Action** at the default value of **Auto**
- Set the **Replace Action** for the **Request-Line** Header to **Overwrite** and set the **Overwrite Value** to the Completel domain name. In test **trusted.voip.completel.fr** was used.

![Topology Hiding Profiles: Completel](image)

### 7.9. Signalling Rules

Signalling rules are a mechanism on Avaya SBCE to handle any unusual signalling scenarios that may be encountered for a particular Service Provider. In the case of Completel, the network is sending a re-INVITE to change the codec for fax calls to T.38 after the enterprise has already sent its own re-INVITE. This is causing the enterprise to send a “491 Request Pending - another fax request in progress” message. When the network receives this message, it is clearing the call. Signalling Rules can be used to convert the 491 message to a 200 OK which prevents the network from clearing the call.

In addition to the above scenario, signalling rules can be used to convert the network response to **OPTIONS**, which is “503 Not Implemented – Fake Return Code”, to a 200 OK which is accepted by Session Manager. They can also be used to remove proprietary headers from the SIP messages coming from the enterprise.
During test, signalling rules were used on both Session Manager and Completel network. The signalling rule on Session Manager was used to remove proprietary headers. To define the signalling rule, navigate to **Domain Policies ➔ Signalling Rules** in the main menu on the left hand side (not shown). Click on **Add** and enter details in the Signalling Rule pop-up box

- In the **Rule Name** field enter a descriptive name for Session Manager signalling rule and click **Next** and **Next** again, then **Finish** (not shown)
- Click on the **Request Headers** tab and then click on **Add In Header Control** (not shown)
- Check the **Proprietary Request Header** box
- Enter the name of the proprietary header in the Header Name field, in the example shown **P-Site** is used and **ALL** in the Method Name field
- Check **Forbidden** in the Header Criteria options
- In the **Presence Action** drop down menu, select **Remove Header**
- Click **Finish**

![Add Header Control](image)

**Note:** the above is an example of the proprietary headers. During test, the same was done for **P-AV-Message-Id**, **P-Charging-Vector** and **P-Location** headers.

When finished, all the Request Headers defined will be shown under the Request Headers tab as shown in the screenshot.
The signalling rule on the Completel network was used to change the responses to “SIP OPTIONS” messages and the “491 Request Pending - another fax request in progress” messages. To define the signalling rule, navigate to **Domain Policies → Signalling Rules** in the main menu on the left hand side. Click on **Add** and enter details in the Signalling Rule pop-up box (not shown)

- In the **Rule Name** field enter a descriptive name for the Completel network signalling rule and click **Next** and **Next** again, then **Finish** (not shown)
- Click on the **Responses** tab and then click on **Add Out Response Control** (not shown)
- In the **Response Code** drop down box, select **491**
- In the **Method Name** enter the method of the original request, in this case **INVITE**
- In the **Dialog Action** drop down box, select **Change response to**
- In the two **Dialog Action fields**, enter **200** and **OK**
- Click **Finish**

- Click on the **Responses** tab again and this time then click on **Add In Response Control**
- In the **Response Code** drop down box, select **503**
- In the **Method Name**, enter the method of the original request, in this case **OPTIONS**
- In the **Dialog Action** drop down box, select **Change response to**
- In the two **Dialog Action fields**, enter **200** and **OK**
• Click **Finish**

The screenshot for the Response Control for the OPTIONS message is not shown.
When finished, all the Request Headers defined will be shown under the Request Headers tab as shown in the screenshot.

End Point Policy Groups are required to implement the signalling rules. To define one for Session Manager, navigate to Domain Policies → End Point Policy Groups in the main menu on the left hand side. Click on Add and enter details in the Policy Group pop-up box (not shown)

- In the Group Name field enter a descriptive name for the Session Manager Policy Group, in this case SM-def-low, and click Next
- Leave the Application, Border, Media, Security and Time of Day fields at their default values
- In the Signaling drop down menu, select the recently added signalling rule for Session Manager (ASM9)
- Leave the Time of Day field at its default value
To define an End Point Policy Group for the Completel network, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown)

- In the **Group Name** field enter a descriptive name for the Completel network, in this case **Cmptl-def-low**, and click **Next**
- Leave the **Application, Border, Media, Security** and **Time of Day** fields at their default values
- In the **Signaling** drop down menu, select the recently added signalling rule for the Completel network (**Completel**)
- Leave the Time of Day field at its default value

7.10. **Server Flows**

Server Flows combine the previously defined profiles into an outgoing flow from Session Manager to the Completel SBC and an incoming flow from the Completel SBC to Session Manager. This configuration ties all the previously entered information together so that calls can be routed from Session Manager to the Completel SBC and vice versa.
To define a Server Flow for Session Manager, navigate to **Device Specific Settings → End Point Flows**. Click on the **Server Flows** tab. Select **Add Flow** (not shown). Enter details in the pop-up menu.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Session Manager, in this case **Session Manager** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.6** for Session Manager.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Complete network defined in **Section 7.7**.
- In the **End Point Policy Group** drop down menu, select the End Point Policy Group that contains the Signalling Rules for Session Manager defined in **Section 7.9**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.8** and click **Finish**.
<table>
<thead>
<tr>
<th>Flow Name</th>
<th>Session Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Configuration</td>
<td>ASM9_Call_Server</td>
</tr>
<tr>
<td>URI Group</td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td></td>
</tr>
<tr>
<td>Remote Subnet</td>
<td></td>
</tr>
<tr>
<td>Received Interface</td>
<td>Ext_Sig</td>
</tr>
<tr>
<td>Signaling Interface</td>
<td>Int_Sig</td>
</tr>
<tr>
<td>Media Interface</td>
<td>Int_Med</td>
</tr>
<tr>
<td>End Point Policy Group</td>
<td>SM-defFlow</td>
</tr>
<tr>
<td>Routing Profile</td>
<td>Trunk_Server</td>
</tr>
<tr>
<td>Topology Hiding Profile</td>
<td>ASM9</td>
</tr>
<tr>
<td>File Transfer Profile</td>
<td>None</td>
</tr>
</tbody>
</table>

Finish
To define a Server Flow for the Completel network, navigate to **Device Specific Settings ➔ End Point Flows**. Click on the **Server Flows** tab. Select **Add Flow** (not shown). Enter details in the pop-up menu.

- In the **Name** field enter a descriptive name for the server flow for the Completel network, in this case a generic name of **Trunk Server** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.6** for the Completel network.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Completel network is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Completel network is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for the Completel network is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.7**.
- In the **End Point Policy Group** drop down menu, select the End Point Policy Group that contains the Signalling Rules for Completel defined in **Section 7.9**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Completel network defined in **Section 7.8** and click **Finish**.
The information for all Server Flows is shown on a single screen on Avaya SBCE.
8. Configure Completel Equipment
The configuration of the Completel equipment used to support the Completel UCM service is outside of the scope of these Application Notes and will not be covered. To obtain further information on Completel equipment and system configuration please contact an authorised Completel representative.
9. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager Home tab click on Session Manager and navigate to Session Manager ➤ System Status ➤ SIP Entity Monitoring (not shown). Select the relevant SIP Entity from the list and observe if the Conn Status and Link Status are showing as up.

![SIP Entity, Entity Link Connection Status](image)

2. From Communication Manager SAT interface run the command status trunk n where n is a previously configured SIP trunk. Observe if all channels on the trunk group display in-service/idle.

```
status trunk 2
```

<table>
<thead>
<tr>
<th>Member</th>
<th>Port</th>
<th>Service State</th>
<th>Mtce Connected Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001/001</td>
<td>T00001</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/002</td>
<td>T00002</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/003</td>
<td>T00003</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/004</td>
<td>T00004</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/005</td>
<td>T00005</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/006</td>
<td>T00006</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/007</td>
<td>T00007</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/008</td>
<td>T00008</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/009</td>
<td>T00009</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/010</td>
<td>T00010</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
</tbody>
</table>

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Should issues arise with the SIP trunk, use Avaya SBCE trace facility to check that the REGISTER requests sent from Avaya SBCE are receiving a response.

To define the trace, navigate to Device Specific Settings ➔ Advanced Options ➔ Troubleshooting ➔ Trace in the main menu on the left hand side and select the Packet Capture tab.

- Select the SIP Trunk interface from the Interface drop down menu
- Select the signalling interface IP address from the Local Address drop down menu
- Enter the IP address of the Service Provider’s SBC in the Remote Address field or enter a * to capture all traffic
- Specify the Maximum Number of Packets to Capture, 10000 is shown as an example
- Specify the filename of the resultant pcap file in the Capture Filename field
- Click on Start Capture

To view the trace, select the Captures tab and click on the relevant filename in the list of traces.
The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response in the form of a 200 OK will be seen from the Service Provider.

10. Conclusion
These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.2 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to the Completel UCM service. Completel UCM is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in Section 2.2.

11. Additional References
This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at [http://support.avaya.com](http://support.avaya.com).

[12] Administering Avaya Aura® Session Manager Release 6.3, June 2013,